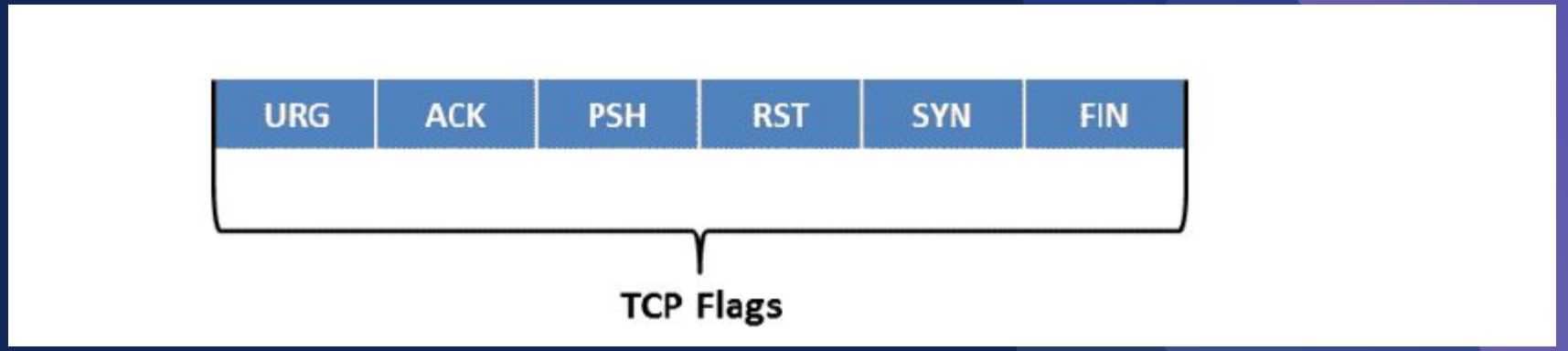
Overview of Network Scanning

- Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine.

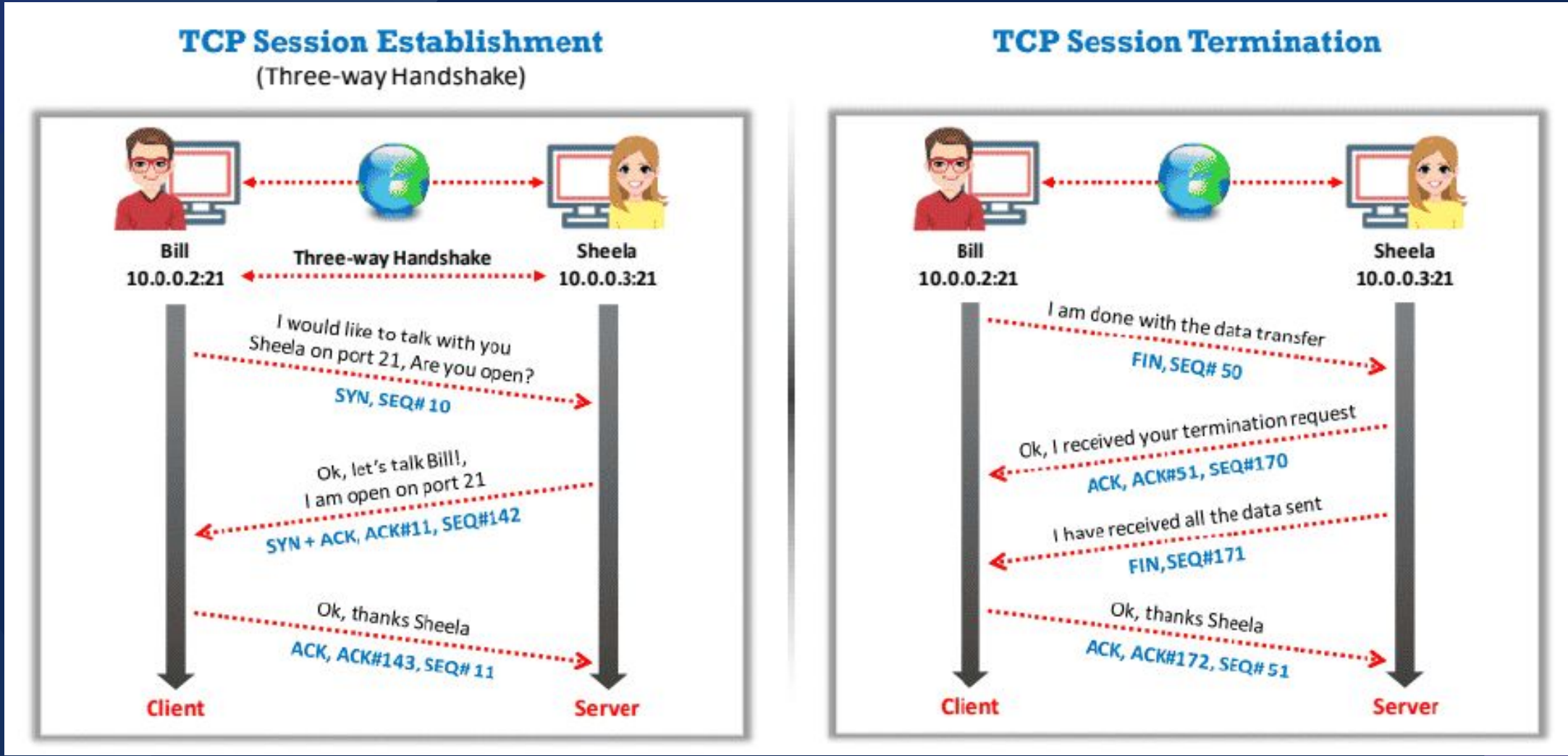
- The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and track the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more information about the target system to determine the presence of any configuration lapses. The attacker then uses the information obtained to develop an attack strategy.

TCP Communication

The TCP header contains various flags that control the transmission of data across a TCP connection. Six TCP control flags manage the connection between hosts and give instructions to the system. Four of these flags (SYN, ACK, FIN, and RST) govern the establishment, maintenance, and termination of a connection. The other two flags (PSH and URG) provide instructions to the system. The size of each flag is 1 bit. As there are six flags in the TCP Flags section, the size of this section is 6 bits. When a flag value is set to "1," that flag is automatically turned on.



Three way handshake mechanism



Network Scanning Tools

- NMAP & Zenmap
  - Syntax: # nmap <options> <Target IP address>
- Hping3
  - Syntax: # hping3 <options> <Target IP address>
- NetScanTools Pro
  - Source: https://www.netscantools.com
- IP Scanner (used from mobile)
  - Source: https://10base-t.com

Host discovery

- List Scan
  - dig google.com
  - nmap -sL <IP>
- Ping Scan
  - nmap -sn <IP>
  - nmap -PE -sn <IP> (Pure ICMP Ping)
- UDP Scan
  - nmap -sn -PU <IP>
- ARP Scan
  - nmap -sn -PR <IP>
- Basic port scan
  - nmap -sS -Pn <IP>

OS Discovery/ Banner grabbing

Banner grabbing, or "OS fingerprinting," is a method used to determine the OS that is running on a remote target system.

Active Banner Grabbing

Active banner grabbing applies the principle that an OS's IP stack has a unique way of responding to specially crafted TCP packets. This happens because of different interpretations that vendors apply while implementing the TCP/IP stack on a particular OS.

Passive Banner Grabbing

Like active banner grabbing, passive banner grabbing also depends on the differential implementation of the stack and the various ways in which an OS responds to packets. However, instead of relying on scanning the target host, passive fingerprinting captures packets from the target host via sniffing to study telltale signs that can reveal an OS.

- nmap –O <target>
- nmap –sV <target>

Scanning beyond IDS & Firewall

- Though firewalls and IDSs can prevent malicious traffic (packets) from entering a network, attackers can manage to **send intended packets to the target** by **evading an IDS or firewall** through the following techniques:

1. Packet Fragmentation
2. Source Routing
3. Source Port Manipulation
4. IP Address Decoy
5. IP Address Spoofing
6. MAC Address Spoofing
7. Creating Custom Packets
8. Randomizing Host Order and Sending Bad Checksums
9. Proxy Servers
10. Anonymizers

Network Scanning countermeasures

Ping Sweep countermeasures:

- Configure the firewall to detect and prevent ping sweep attempts instantaneously.
- Use intrusion detection systems (IDSes) and intrusion prevention systems (IPSes), such as Snort (https://www.snort.org), to detect and prevent ping-sweep attempts.
- Carefully evaluate the type of Internet Control Message Protocol (ICMP) traffic flowing through enterprise networks.
- Terminate the connection with any host sending more than 10 ICMP ECHO requests.

Banner grabbing countermeasures:

- Display false banners to mislead or deceive attackers.
- Turn off unnecessary services on the network host to limit information disclosure.
- Use server masking tools to disable or change banner information.

IP spoofing countermeasures:

- Firewall and traffic filtering